CLAIMS

What is claimed is:

1. A method comprising:

receiving a decoded scrambling key having a key size according to a first cryptographic protocol;

reducing the key size of the decoded scrambling key to match a key size of a second cryptographic protocol to form a reduced key size descrambling key whose value is a function of every bit of the decoded scrambling key; and

descrambling received scrambled content according to the reduced key size descrambling key.

2. The method of claim 1, wherein reducing the key size comprises:

dividing the decoded scrambling key into a lower M-bits and an upper N-bits;

performing a logical exclusive OR operation of the upper N-bits across the lower M-bits to form an M-bit descrambling key as the reduced key size descrambling key.

3. The method of claim 1, wherein reducing the key size comprises:

dividing the decoded descrambling key into a lower M-bits and an upper M-bits;

performing a logical XOR operation on the lower M-bits and the upper M-bits to form an M-bit descrambling key as the reduced key size descrambling key.

4. The method of claim 1, wherein reducing the key size comprises:

dividing the decoded descrambling key into a lower M-bits and an upper M-bits;

performing a logical exclusive OR operation on the lower M-bits and the upper M-bits to form an M-bit descrambling key;

dividing the M-bit descrambling key into a lower X-bits and an upper Y-bits; and

performing a logical exclusive OR operation of the upper Y-bits across the lower X-bits to form an X-bit descrambling key as the reduced key size descrambling key.

5. The method of claim 1, wherein reducing the key size comprises:

hashing the bits of the decoded scrambling key; and

selecting bits from the hash to form the reduced key size descrambling key.

6. The method of claim 1, wherein the first cryptographic protocol is an advanced encryption standard protocol and the second cryptographic protocol is one of a triple data encryption standard protocol (3DES), a digital video broadcast (DVB) common scrambling algorithm (CSA) and a data encryption standard (DES) algorithm.

7. The method of claim 1, wherein the first cryptographic protocol is a triple data encryption standard protocol (3DES) and the second cryptographic protocol is one of a digital video broadcast (DVB) common scrambling algorithm (CSA) and a data encryption standard (DES) algorithm.

8. The method of claim 1, wherein the first cryptographic protocol is digital video broadcast (DVB) common scrambling algorithm (CSA) and the second cryptographic protocol is the data encryption standard (DES) algorithm.

9. An article of manufacture including a machine readable medium having stored thereon instructions which may be used to program a system to perform a method, comprising:

receiving a decoded scrambling key having a key size according to a first cryptographic protocol to form a reduced key size descrambling key;

reducing the key size of the decoded scrambling key to match a key size of a second cryptographic protocol whose value is a function of every bit of the decoded scrambling key; and

descrambling received scrambled content according to the reduced key size descrambling key.

10. The article of manufacture of claim 9, wherein reducing the key size comprises:

dividing the decoded scrambling key into a lower M-bits and an upper N-bits;

performing a logical exclusive OR operation of the upper N-bits across the lower M-bits to form an M-bit descrambling key as the reduced key size descrambling key.

11. The article of manufacture of claim 9, wherein reducing the key size comprises:

dividing the decoded descrambling key into a lower M-bits and an upper M-bits;

performing a logical exclusive OR operation on the lower M-bits and the upper M-bits to form an M-bit descrambling key as the reduced key size descrambling key.

12. The article of manufacture of claim 9, wherein reducing the key size comprises:

dividing the decoded descrambling key into a lower M-bits and an upper N-bits;

performing a logical exclusive OR operation on the lower M-bits and the upper N-bits to form an M-bit descrambling key;

dividing the M-bit descrambling key into a lower X-bits and an upper Y-bits; and

performing a logical exclusive OR operation of the upper Y-bits across the lower X-bits to form an X-bit descrambling key as the reduced key size descrambling key.

13. The article of manufacture of claim 9, wherein the first cryptographic protocol is an advanced encryption standard protocol and the second cryptographic protocol is one of a triple data encryption standard protocol (3DES), a digital video broadcast (DVB) common scrambling algorithm (CSA) and a data encryption standard (DES) algorithm.

14. The article of manufacture of claim 9, wherein reducing the key size comprises:

hashing the bits of the decoded scrambling key; and

selecting bits from the hash to form the reduced key size descrambling key.

15. The article of manufacture of claim 9, wherein the first cryptographic protocol is a triple data encryption standard protocol (3DES) and the second cryptographic protocol is one of a digital video broadcast (DVB) common scrambling algorithm (CSA) and a data encryption standard (DES) algorithm.

16. The article of manufacture of claim 9, wherein the first cryptographic protocol is digital video broadcast (DVB) common scrambling algorithm (CSA) and the second cryptographic protocol is the data encryption standard (DES) algorithm.

17. An integrated circuit comprising:

a first cryptographic block that may be iterated without limit to descramble received information using one of an internal key and a preprogrammed key to form one of a descrambled key and descrambled data;

a key feedback path to store the descrambled key as an internal key and to provide the one of the internal key and the preprogrammed key to a key input of the first cryptographic block; and

a second cryptographic block to descramble received scrambled digital content using a final descrambling key from the first cryptographic block to form descrambled digital content.

18. The integrated circuit of claim 17, further comprising:

a data feedback path to store the descrambled data within a data register as internal data;

data selection logic coupled to the data register and an external information input, the data selection logic to provide one of internal data from the data register and received information from the external information input to a data input of the first cryptographic block.

19. The integrated circuit of claim 17, wherein the key feedback path further comprises:

a preprogrammed key register to store at least the preprogrammed key;

an internal key register to store at least the descrambled key; and

key selection logic to provide the one of the preprogrammed key and the internal key to the key input of the first cryptographic block using controls accessible outside the integrated circuit and accessible by an insecure CPU.

20. The integrated circuit of claim 17, further comprising:

gate enable logic coupled to the key feedback path of the first cryptographic block to receive the one of the internal key and the preprogrammed key; and

a logic gate coupled to a data output of the first cryptographic block, the logic gate to compute a key hash value from the one of the internal key and the preprogrammed key received from the gate enable logic and the descrambled key received from the data output of the first cryptographic block when enabled by the gate enable logic.

21. The integrated circuit of claim 17, further comprising:

gate enable logic coupled to the data input of the first cryptographic block to receive the received information; and

a logic gate coupled to a data output of the first cryptographic block, the logic gate to compute a hash data value from the received information and the descrambled data from the data output of the first cryptographic block when enabled by the gate enable logic.

22. The integrated circuit of claim 17, further comprising:

a data feedback path to store at least the descrambled data within a data register;

gate enable logic coupled to the data register; and

a logic gate coupled to a data input of the first cryptographic block, the logic gate to form a permuted value from the received information and the descrambled data from the gate enable logic and to provide the permuted value to the data input of the first cryptographic block when enabled by the gate enable logic and to provide the received information to the data input of the first cryptographic block when disabled.

23. The integrated circuit of claim 17, further comprising:

gate enable logic to receive an internal data value;

a logic gate coupled to the key feedback path of the first cryptographic block and the gate enable logic, the logic gate to compute a permuted key value from the internal data value and the one of the internal key and the preprogrammed key when enabled by the gate enable logic and to provide the permuted key value to the key input of the first cryptographic block; and

an external data register coupled to a data output of the first cryptographic block to store descrambled data generated by the first cryptographic block with the permuted key value received as the key input of the first cryptographic block.

24. The integrated circuit of claim 17, wherein the first cryptographic block is an embedded cryptographic CPU programmed to iteratively descramble the received information using one of the internal key and the preprogrammed key to form one of the descrambled key and descrambled data; and

wherein the key feedback path and a data feedback path to operate according to an off-chip insecure CPU.

25. The integrated circuit of claim 18, wherein the key feedback path and the data feedback path to operate according to an off-chip insecure CPU.

26. The integrated circuit of claim 17,

wherein the first cryptographic block is to operate according to a state machine; and

wherein the key feedback path and a data feedback path to operate according to an off-chip insecure CPU.

27. The integrated circuit of claim 23, wherein the internal value being one of a fixed value, a stored internal key, stored internal data, and a one-time-programmable value.

28. The integrated circuit of claim 17, further comprising:

gate enable logic to receive an internal data value;

a logic gate coupled to the key feedback path of the first cryptographic block and the gate enable logic, the logic gate to compute a permuted key value from the internal data value and the one of the internal key and the preprogrammed key when enabled by the gate enable logic and to provide the permuted key value to the key input of the first cryptographic block to generate the final key and to provide the final key as a key input of the second cryptographic block.

29. The integrated circuit of claim 28, wherein the internal value being one of a fixed value, a stored internal key, stored internal data, and a one-time-programmable value.

30. The integrated circuit of claim 17, further comprising:

a logic gate to receive the descrambling key from the first cryptographic block and an internal value, the logic gate to generate a permuted key value as the final key and provide the final key to a key input of the second cryptographic block.

31. The integrated circuit of claim 30, wherein the internal value being one of a fixed value, a stored internal key, stored internal data, and a one-time-programmable value.

32. The integrated circuit of claim 17, further comprising:

key reduction logic to receive the descrambled key from the first cryptographic block having a key size according to a first cryptographic protocol of the first cryptographic block, the key reduction logic to reduce the key size of the descrambled key to match a key size of a second cryptographic protocol of the second cryptographic block to form the final key whose value is a function of every bit of the descrambled key.

33. The integrated circuit of claim 32, wherein the first cryptographic protocol is an advanced encryption standard (AES) protocol and the second cryptographic protocol is one of a triple data encryption standard (3DES) protocol, a digital video broadcast (DVB) common scrambling algorithm (CSA) protocol and a data encryption standard (DES) protocol.

34. The integrated circuit of claim 32, wherein the first cryptographic protocol is a triple data encryption standard protocol (3DES) and the second cryptographic protocol is one of a digital video broadcast (DVB) common scrambling algorithm (CSA) and a data encryption standard (DES) algorithm.

35. The integrated circuit of claim 32, wherein the first cryptographic protocol is digital video broadcast (DVB) common scrambling algorithm (CSA) and the second cryptographic protocol is the data encryption standard (DES) algorithm.

36. The integrated circuit of claim 17, wherein the integrated circuit is a decoder integrated circuit to decompress the descrambled digital content .

37. The integrated circuit of claim 17, wherein the integrated circuit is a cryptographic integrated circuit.

38. The integrated circuit of claim 17, further comprising:

a decoder to decode the descrambled digital content to form clear digital content.

39. The integrated circuit of claim 38, further comprising:

a non-volatile memory to store the clear digital content in a scrambled format.

40. The integrated circuit of claim 17, wherein the preprogrammed key is a one-time programmable value that cannot be read or overwritten once programmed.

41. A set-top box, comprising:

a tuner to receive scrambled content;

a CPU; and

an integrated circuit select at least one of a preprogrammed key, internal key, external data and internal data under control of the CPU, comprising:

a first cryptographic block to descramble received information using one of an internal key and a preprogrammed key to form one of a descrambled key and descrambled data,

a key feedback path to iteratively store the descrambled information as one of an internal key and internal data, and to provide the one of the internal key and the preprogrammed key to a key input of the first cryptographic block and to provide the one of external data and the internal data to a data input of the first cryptographic block,

a second cryptographic block to descramble received scrambled digital content using a final descrambling key from the first cryptographic block to form descrambled digital content, and

a decoder to decode the descrambled digital content to form clear digital content.

42. The set-top box of claim 41, further comprising:

a data feedback path to store the descrambled data within a data register as internal data;

data selection logic coupled to the data register and an external information input, the data selection logic to provide one of internal data from the data register and received information from the external information input to a data input of the first cryptographic block.

43. The set-top box of claim 41, wherein the key feedback path further comprises:

a preprogrammed key register to store at least the preprogrammed key;

an internal key register to store at least the descrambled key; and

key selection logic to provide the one of the preprogrammed key and the internal key to the key input of the first cryptographic block.

44. The set-top box of claim 41, further comprising:

gate enable logic coupled to the key feedback path of the first cryptographic block to receive the one of the internal key and the preprogrammed key; and

a logic gate coupled to a data output of the first cryptographic block, the logic gate to compute a key hash value from the one of the internal key and the preprogrammed key received from the gate enable logic and the descrambled key received from the data output of the first cryptographic block when enabled by the gate enable logic.

45. The set-top box of claim 41, further comprising:

gate enable logic coupled to the data input of the first cryptographic block to receive the received information; and

a logic gate coupled to a data output of the first cryptographic block, the logic gate to compute a hash data value from the received information and the descrambled data from the data output of the first cryptographic block when enabled by the gate enable logic.

46. The set-top box of claim 41, further comprising:

a data feedback path to store at least the descrambled data within a data register;

gate enable logic coupled to the data register; and

a logic gate coupled to a data input of the first cryptographic block, the logic gate to form a permuted value from the received information and the descrambled data from the gate enable logic and to provide the permuted value to the data input of the first cryptographic block when enabled by the gate enable logic and to provide the received information to the data input of the first cryptographic block when disabled.

47. The set-top box of claim 41, further comprising:

gate enable logic to receive an external data value;

a logic gate coupled to the key feedback path of the first cryptographic block and the gate enable logic, the logic gate to compute a permuted key value from the external data value and the one of the internal key and the preprogrammed key when enabled by the gate enable logic and to provide the permuted key value to the key input of the first cryptographic block; and

an external data register coupled to a data output of the first cryptographic block to store descrambled data generated by the first cryptographic block with the permuted key value received as the key input of the first cryptographic block.

48. The set-top box of claim 41, wherein the first cryptographic block and the second cryptographic block are logic operating in accordance with an advanced encryption standard (AES).

49. The set-top box of claim 41, further comprising:

a non-volatile memory to store the clear digital content in a scrambled format.

50. The set-top box of claim 41, wherein the preprogrammed key is a one-time programmable value that cannot be read or overwritten once programmed.